Gutsalyuk, Mykhaylo V.
Klymenko, Olga A.

Combate à criminalidade cibernética e garantias de segurança cibernética na Ucrânia

http://hdl.handle.net/11067/3789
https://doi.org/10.34628/ge3j-wn63

COMBATE À CRIMINALIDADE CIBERNÉTICA E GARANTIAS DE SEGURANÇA CIBERNÉTICA NA UCRÂNIA

Mykhaylo V. Gutsalyuk
doutorado em direito(PhD), docente
Kyiv, Ucrânia

Olga A. Klymenko
doutorada em direito (PhD)
Centro Lusíada de investigação em Política Internacional e Segurança (CLIPIS)
Kyiv, Ucrânia

Resumo: O artigo analisa as questões de segurança informática e combate ao crime cibernético. Propõem-se as diretrizes de aprimoramento da legislação atual no domínio referido e elaboração do segmento seguro *ID-web – Internet*.

Palavras-chave: Crime cibernético, Segurança cibernética, Cooperação internacional, *ID-web*.

Abstract: The article deals with the issues of Cybersecurity and Cybercrime. The improvement of the legislation in this area and the introduction of safe ID-web Internet are proposed.

Keywords: Cybercrime, Cybersecurity, International cooperation, ID-web.

Introdução

O número total de utilizadores da Internet continua a crescer e já ultrapassou os 3.4 bilhões.[1] A expansão em larga escala de tecnologias de informação e comunicação, praticamente em todos os domínios da vida, causou o impacto significativo sobre o desenvolvimento dinâmico da economia global e levou á necessidade de reforçar a segurança internacional. Estas tecnologias avançadas proporcionam oportunidade de obter os benefícios económicos e sociais enormes. Ao mesmo tempo, estes podem ser usados para fins criminosos, incompatíveis com manutenção de segurança, o que resultou nos últimos anos em aumento significativo do nível de risco de propagação da atividade criminal cibernética internacional.

Os peritos do Fórum Mundial Econômico em Davos elaboraram e publicaram em janeiro de 2017 o relatório anual "Global Risks Report 2017", sobre os riscos globais a nível mundial. Com base nos conceitos nele apresentados, entre os mais importantes para a comunidade mundial, nomeadamente no terceiro lugar, destacam-se os riscos tecnológicos – o roubo de identidade, manipulação de dados pessoais, ataques cibernéticos e crimes cibernéticos de grande escala.[2]

As pesquisas realizadas pela Europol estimulam, que os prejuízos anuais de estados-membros da EU, causados por cibercriminalidade, ascendem a 265 bilhões de euros. Para a economia mundial este valor aproxima-se aos 900 bilhões de euros. E este é apenas o lado financeiro do problema.[3]

Com base no panorama atual, merece atenção a opinião do ex-adjunto do Procurador-Geral em questões de segurança nacional do Ministério da Justiça de EUA John Carlin, que aponta para uma das tendências de propagação de ameaças cibernéticas nos próximos 3 - 5 anos – crimes cibernéticos cometidos com o apoio do estado, e ataques realizados por espiões cibernéticos cujo objetivo é o benefício financeiro.[4] Essa informação foi confirmada pelo Secretário-geral do NATO Jens Stoltenberg, que durante uma conferência de imprensa em Bruxelas, em 15 de Fevereiro de 2017, afirmou, que Aliança enfrenta sérios ataques cibernéticos, levados a cabo pelos hackers, que operam não só em interesses próprios, mas também para o benefício do Estado agressor.[5]

Atualmente, a atenção particular merece a possibilidade de cometimento de atos terroristas com o uso de tecnologias de informação e comunicação nas infraestruturas críticas ou estruturas militares.

Por exemplo, de acordo com o relatório do centro analítico do BASIC (British American Security Information Council), os submarinos britânicos Trident são vulneráveis a ataques cibernéticos. Um ataque bem-sucedido pode "neutralizar o controlo, levar á morte de pessoas, derrota, ou, possivelmente, á troca catastrófica de ataques nucleares" – diz o relatório.[6]

Em 2015 e 2016 foram realizados vários ataques cibernéticos no setor financeiro e energético da Ucrânia, que resultaram em consequências prejudiciais – centenas milhares de pessoas ficaram sem eletricidade durante longos períodos de tempo. A investigação levada a cabo por empresa Dragos atribui a culpa aos hackers. Eles desenvolveram o vírus CrashOverRride, que impercetivelmente penetra no sistema co computador, e depois ativa-se simultaneamente em vários lugares e pode controlar os interruptores de centrais e subestações elétricas. Isso permite aos hackers simplesmente desligar o fornecimento de eletricidade ou danificar o equipamento. A versão atualizada do CrashOverRide pode vir a ser utilizada contra as redes elétricas , e isso levará á efeito devastador.[7]

A questão de segurança de objetos de infraestrutura crítica foi analisada no dia 13 de Fevereiro de 2017 durante a presidência da Ucrânia no Conselho de Segurança da ONU, onde foi adotada a respetiva Resolução N.º 2341 (2017). O documento afirma, que o Conselho de Segurança da ONU recomenda:

- inteirar a informação acerca de problemas criadas pelos ataques terroristas direcionados contra objetos de infraestrutura crítica;
- incentiva todos os países aperfeiçoar as suas estratégias de redução de riscos de estes ataques;
- fortalecer as parcerias públicas e privadas com objetivo de trocar as informações e experiencias de recuperação apos de danos sofridos.

Ao mesmo tempo, todos os Estados, que tem as capacidades de fazê-lo, devem contribuir para o crescimento do potencial, preparação e assistência técnica, transferência de tecnologias e implementação efetiva do programa, para que todos os Estados pudessem alcançar proteção de infraestrutura crítica contra ataques terroristas.[8]

A Ucrânia atribui grande importância á questão de segurança cibernética. A fim de criar as condições para o funcionamento seguro do espaço cibernético, a sua utilização para o benefício de pessoas, da sociedade e do Estado foi elaborada e aprovada a Estratégia de Segurança Cibernética da Ucrânia (Decreto do Presidente da Ucrânia N.º 96/2016 de 15 de Março de 2016).[9]

O Decreto do Presidente da Ucrânia N.º 32/2017 de 13 de Fevereiro de 2017 aprovou a decisão do Conselho de Segurança Nacional e Defesa da Ucrânia "Ameaças á segurança cibernética do Estado e medidas de emergência para combatê-las". O documento definiu os objetivos instantâneos e a curto prazo do Gabinete de Ministros da Ucrânia e de agências de aplicação da lei sobre a

proteção de informação em sistemas de informação e de telecomunicações, e em particular, nos objetos de infraestruturas críticas.[10]

As questões problemáticas de combate á criminalidade cibernética na Ucrânia foram estudadas pelos investigadores nacionais, entre quais os autores destacam N. M. Akhtyrs´ka, P. D. Bilenchuk, K. I. Beliakov, V. M. Butuzov, V. D. Havrylovs´kyi, M. A. Pohorets´kyi, V. H. Hahanovs´kyi, V. P. Shelomencev, O. M. Yurchenko e outros. No entanto, o desenvolvimento rápido de tecnologias da informação e de formas e meios de atividades ilegais no espaço cibernético requere ademais pesquisas.

O **objetivo** do presente artigo foi continuar o estudo sobre atividades ilegais no sistema global de redes, Internet, e fornecer as sugestões para melhorar a segurança no segmento ucraniano da Internet.

Resumo das principais normas

Devido a crescente escala de criminalidade cibernética, a fim de desenvolver os mecanismos legais de combate às ameaças a redes de computadores, em maio de 2011 a União Internacional das Telecomunicações e o Gabinete das Nações Unidas contra a Droga e Crime assinaram o acordo sobre o combate contra a criminalidade cibernética. Para a adoção de medidas específicas, destinadas a reduzir as ameaças às computadores, a ONU desenvolveu o Programa de Segurança Cibernética Global,que identificou os cinco domínios principais:[11]

1 – medidas legais;
2 – medidas técnicas e processuais;
3 – estrutura organizacional;
4 – programas de treino/melhoria de competência;
5 – cooperação internacional.

Ausência de fronteiras internacionais é a característica principal do espaço cibernético. Por este motivo, a regulamentação legal das relações sociais, que surgem na deteção e investigação de atividade ilegal, ganha a importância particular. O criminoso pode permanecer no território de um Estado, iniciar o ataque cibernético com o uso de um sistema informático situado no território do outro Estado, e causar os danos á pessoa ou entidade localizada em um país terceiro. Ao mesmo tempo, os programas maliciosos podem atravessar mais fronteiras, sem alertar as autoridades públicas competentes.

Por exemplo, ataque de vírus "Wanna Cry" em larga escala, que teve lugar nos dias 12 – 13 de maio de 2017 atingiu desenhas de milhares de computadores em todo o mundo. Na sequência, uma rede de estabelecimentos médicos do Reino Unido foi forçada a recusar prestação de serviços aos pacientes, mesmo

em casos de emergência, devido ao fracasso dos sistemas de computadores[12]. Em Espanha foram atacados o Departamento de Energia e empresa de telecomunicações "Telefónica". Na Alemanha foram infetados os computadores de centros de controlo de uma empresa ferroviária, e isso resultou em avaria de sistemas de supervisão.[13] Em França, a produtora de automóveis "Renault" sofreu um ataque muito forte.[14] Em Portugal a maior provedora de serviços de telecomunicações "Portugal Telecom" sofreu os danos significativos. Segundo a ONG "JPCERT" no Japão os ataques dos hackers atingiram pelo menos dois mil computadores, entre eles encontrava-se a rede de computadores de um hospital privado, que estava completamente bloqueada. Na Coreia de Sul foi atacada a maior rede de cinemas de país. Os relatórios informam, que na China os ataques de criminosos cibernéticos atingiram aproximadamente 15% de redes de instituições de ensino. Alem disso, foram danificados os sistemas de computadores de centros comerciais e de escritórios, hospitais, postos de abastecimento de combustível, correios, estações ferroviárias e escritórios estaduais.[15]

Segundo a informação da empresa KnowBe4, os danos, causados por vírus "WannaCry" durante os primeiros quatro dias, ultrapassam um bilhão de dólares americanos.[16]

O relatório anual da Europol sobre avaliação de ameaças de crimes cibernéticos identifica as seguintes tendências principais no domínio da criminalidade cibernética da EU:

1. Eliminação por programas de extorsão de outros softwares mal-intencionados, como por exemplo trojans bancários, uma vez que os programas de extorsão tornam-se uma ameaça principal para indivíduos e empresas;
2. Comercialização de serviços criminais (crime-as-a-service). O "mercado negro" de crimes informáticos oferece uma vasta gama de bens e serviços: conjuntos de explorações, dados pessoais roubados, informações de cartões de crédito, informações sobre servidores comprometidos, venda e aluguer de botnets, serviços para realizar os ataques informáticos de género "ataque de negação de serviço" (ataques DDos), serviços de invasão de redes de computadores;
3. O uso ativo por criminosos (e organizações terroristas) para ocultar atividades ilegais de motores de busca invisíveis (darknet), meios de despersonalização (anonimatos), codificação de dados, mecanismos de proteção de comunicações e transações, métodos de esteganografia, criptomoedas (bitcoin), o que, por sua vez, complica significativamente o decorrer de investigações judiciais do cibercrime;
4. A emergência de grupos de crime organizado, que utilizam dados de cartões de pagamento comprometidos na base de tecnologia NFC (Near Field Communication). Vários grupos desenvolvem e implementam softwares,

que permitem carregar os dados de cartões NFC-comprometidos para o seu dispositivo e usá-las para pagar as compras ou serviços em lojas que aderiram á tecnologia NFC. Isso é uma indicação de rápida adaptação de criminosos às novas tecnologias, que começam a ser usados para fins ilícitos;

5. Aparecimento em massa de campanhas de phishing, onde o envio de cartas em nome de diretores de grandes empresas (CEO fraude) está usado como o elemento de engenharia social. Este tipo de phishing pode levar á danos significativos (financeiros, reputacionais) de empresa-alvo;
6. Aumento de intensidade e complexidade de ataques DDoS. Em 2015 a maior intensidade do ataque DDoS atingiu 300Gb/s, em 2016 já foram registadas os ataques com trafego superior ao 600Gb/s;
7. Os dados pessoais continuam ser o produto-chave de transgressores. Ataques, cujo objetivo é o roubo de dados, são destinados principalmente à obtenção de informação financeira, registos médicos e dados de propriedade intelectual. Em maioria de situações os dados estão criptografados para poder exigir a redenção;
8. O bitcoin continua a ser uma ferramenta muito usada pelos criminosos de informática em pagamento de serviços e para receber os resgates de vitimas de programas de extorsão;
9. As aplicações maliciosos para dispositivos móveis, por sua natureza, complexidade e modo de partilha estão cada vez mais próximos às semelhantes de computadores portáteis;
10. Devido ao boom do grooming online e técnicas de engenharia social as vítimas principais de extorsão e abuso sexual são as crianças;
11. A implementação pelas instituições financeiras de mecanismos de segurança, por exemplo chip´s de cartões bancários, ou bloqueio de transações em determinadas áreas geográficas etc, atualmente permite reduzir o número de ações fraudulentas com cartões bancários na EU, e obriga os criminosos realizar os esquemas em outras regiões (América do Norte e do Sul, Sudoeste Asiático). Ao mesmo tempo, o número de ataques á caixas de multibanco continua a aumentar;
12. Aparecimento de novos meios para ataque a computadores devido ao aumento do número de dispositivos conectados, da área "Internet das coisas" (WEBcamaras, televisões, impressoras, roteadores pessoais).[17]

Os confrontos no espaço cibernético, que se assemelham às ações militares, ocorrem a nível de estados. Em 2006 foi criada a primeira unidade militar cibernética do mundo – Air Force Ciber Command, transformada em 2009 em U.S. Army Cyber Command, estrutura de forças armadas de EUA cujo objetivo é a conduta de guerras cibernéticas.[18]

A criação do comando cibernético de EUA intensificou as atividades da área nos outros países. Em Dezembro de 2009 a Coreia do Sul anunciou a criação de uma unidade de tropas cibernéticas. O Centro de Comunicação do governo britânico também começou a preparação ativa de criação de tropas cibernéticas. Em 2010 a China criou uma unidade dedicada a guerra cibernética e segurança da informação. A Federação Russa em 2014 criou as forças militares de operações informáticas para o confronto cibernético com os adversários.

Em 2014, entre 21 e 25 de Maio, ocorreram DDoS ataques e o pirateamento da página de Comissão Eleitoral Central da Ucrânia, durante as eleições presidenciais, isso levou a aparecimento de resultados incorretos na página.

Em Junho de 2014 nos servidores de empresas privadas da Ucrânia e de países da NATO foram detetados os programas maliciosos, que praticavam espionagem. Entre elas encontravam-se Turla/Uurobros/Snake, RedOctober, MiniDuke e NetTreveler.

Em 23 de Dezembro de 2015 por ação do trojan BlackEnergy3 foram desligadas cerca das 30 subestações elétricas de Prykarpattyaoblenergo, e isso deixou mais de 200 mil habitantes da região Ivano Frankivsk sem eletricidade por um período de 1 a 5 horas. Ao mesmo tempo foram executados ataques contra Kyivoblenergo e Tchernivtsioblenergo. No dia 6 de Dezembro de 2016 os hackers atacaram as redes de telecomunicação internas do Ministério das Finanças, Tesouraria e Fundo de Pensões, isso levou a atrasos nos pagamentos orçamentais nos valores acima de centenas milhões de hryvnias.

Em 27 de Junho de 2017 ocorreu o ataque muito abrangente com o uso do programa malicioso, que comprometeu o trabalho de varias empresas privadas e instituições estaduais, como aeroporto Boryspil, Ukrtelecom, central nuclear de Chernobyl, Ukrzaliznytsia etc, também do Gabinete de Ministros e algumas empresas do setor de imprensa. A nível mundial mais de 60 países foram atingidos por este programa, os danos atingem 8 mil milhões de dólares.[19]

Entre os documentos principais, de cariz regulatório e normativo, relativamente ao combate á criminalidade cibernética a nível internacional, inclusivamente organizada, os autores destacam os seguintes:

- Convenção de Nações Unidas Contra o Crime Organizado Transnacional (United Nations Convention against Transnational Ogranized Crime) assinado em Palermo no dia 12 de Dezembro de 2000, e retificado com exceções e advertências por Lei da Ucrânia a partir de 2 de Abril de 2004, N.º 1433 – IV[20];
- Convenção Europeia de Auxilio Judiciário Mutuo em Matéria Penal (European Convention on Mutual Assistance in Criminal Matters) assinado em Estrasburgo em 20 de Abril de 1959, e retificado com exceções e advertências por Lei da Ucrânia a partir de 16 de Janeiro de 1998, N.º 44/98-BP[21];

- Convenção Sobre o Crime Cibernético (Convention on Cybercrime) assinado em 23 de Novembro de 2001 em Budapeste, e retificado com exceções e advertências por Lei da Ucrânia a partir de 7 de Setembro de 2005, N.º 2824-IV.[22]

Juntamente com as medidas normativas e regulatórias, os meios de combate á crime cibernético devem ser acompanhados por objetivos estratégicos de medio e longo prazo. De acordo com esses objetivos os recursos informáticos devem ser protegidos, e responsáveis por elaboração de esquemas criminosos levados á julgamento perante justiça.

Para responder de forma eficaz a crimes cibernéticos relatados, as autoridades necessitam de um quadro jurídico eficiente em ações de investigação e capaz de proporcionar um equilíbrio entre o direito á privacidade e poderes de investigação, disponibilidade operacional e meios de obtenção de provas eletrónicas de fornecedores de serviços de internet, e também garantir a formação adequada e capacidades técnicas de funcionários. Com base na informação acima exposta, os países desenvolvidos formam as unidades especiais de combate á criminalidade cibernética.

Organizações internacionais também adotaram postura ativa relativamente á combate às ameaças cibernéticas. Em Janeiro de 2013 na sede da Europol em Haia (Holanda) iniciou a sua atividade o Centro Europeu sobre Crime Cibernético (European Cibercrime Center – EC3) [3]. Responsável por análise estratégica do estado atual da criminalidade cibernética, definição de política e elaboração da legislação, e também formação de agentes, a atividade do EC3 está direcionada para géneros de crimes cibernéticos seguintes:

- cometidos por grupos criminosos organizados, inclusive aqueles que gerem grandes lucros do crime, como por exemplo fraude na internet;´
- causadores de graves prejuízos ás vitimas, como a exploração sexual online de crianças;
- afetam infraestrutura critica e sistemas informáticos de países da EU, inclusive ataques cibernéticos.

Desde a sua criação EC3 já contribuiu significativamente para o combate contra criminalidade cibernética: participou em dezenas de casos mais emblemáticos, que resultaram em centenas detenções. Colaboradores de EC3 analisaram mais de 800 mil ficheiros, a maioria dos quais eram maliciosos [3].

A fim de combater o crime transnacional, inclusive a investigação de crimes cibernéticos, Estados-membros da EU uniram os esforços e criaram a Organização Europeia de Justiça (Eurojust), cujos poderes estão focados em objetivos seguintes:

- desenvolvimento e melhoria de coordenação entre as autoridades

competentes de países, que participam na investigação e em ação penal no seu próprio território, a ter em consideração qualquer pedido, recebido da autoridade competente de qualquer um deles, ou qualquer informação comunicada por órgão competente com base nas ordens emitidas nos termos de tratados respetivos;
- reforço de colaboração entre as autoridades competentes de países participantes.

Em Junho de 2016, em Bruxelas, a Ucrânia assinou o acordo de cooperação com a Eurojust.[23] Em Dezembro do mesmo ano foi assinado o acordo sobre uma parceria estratégica com a Europol.

Durante os últimos anos a Ucrânia segue o caminho de reforma ativa e a criação de novas estruturas, destinadas a combater a criminalidade cibernética. Em 5 de Outubro de 2015 foi criado o Departamento de Policia Cibernética, uma unidade estrutural da Policia Nacional da Ucrânia, especializada em prevenção, deteção, cessamento e revelação de delitos, de mecanismos de preparação, cuja execução ou encobrimento prevê o uso de computadores, redes de computadores, de telecomunicações ou da Internet.

O Decreto do Presidente da Ucrânia N.º 242/2016 de 7 de Junho de 2016 aprovou a criação do Centro Nacional de Coordenação de Segurança Cibernética, órgão executivo do Conselho Nacional de Segurança e Defesa da Ucrânia, que coordena as atividades dos que asseguram a segurança cibernética.

Ao mesmo tempo, uma serie de tarefas urgentes, definidas pela estratégia de segurança cibernética, permanecem não resolvidas.

Em particular, os autores destacam a incerteza ao nível legislativo de conceitos seguintes: espaço cibernético, crime cibernético, ataque cibernético, objetos de infraestrutura critica etc., que pode causar certos problemas na atividade prática de órgãos policiais, procuradoria e tribunais.[24] É necessário também melhorar o sistema de recolha, analise e avaliação de dados (provas) digitais.

Importância particular adquire a plena implementação da Convenção sobre criminalidade cibernética nos artigos seguintes:

- Artigo 16 – Conservação urgente de dados eletrónicos armazenados;
- Artigo 17 – Conservação urgente e divulgação parcial de dados do trafego de informação;
- Artigo 19 – Busca e apreensão de dados informáticos armazenados;
- Artigo 20 – Recolha de dados sobre o trafego de informação em tempo real;
- Artigo 21 – Interceção do conteúdo de dados da informação.

É conveniente resolver as questões expostas de acordo com a Lei da Ucrânia "Sobre os Princípios Básicos de Preservação de Segurança Cibernética da

Ucrânia", cujo projeto está a ser analisado pelo Conselho Supremo da Ucrânia.

Conclusões. Desde que a Ucrânia adotou em março de 2016 a estratégia de segurança cibernética, o nosso país fez avanços significativos em organização de combate a cibercrime. No entanto, existem varias questões, que precisam de ser resolvidas no futuro mais próximo, entre quais:

- consoante o Acordo de Associação, assinado por Ucrânia, de um lado, e a União Europeia, Comunidade Europeia de Energia Atómica e os seus Estados-membros, por outro lado, é necessário melhorar a legislação atual em conformidade com as disposições da Convenção sobre o cibercrime;
- aprovar as normas legais que definem legalmente a terminologia da criminalidade cibernética;
- desenvolver os mecanismos eficazes de cooperação com o setor privado, principalmente com os prestadores de serviço de internet para efeito de obtenção rápida de dados eletrônicos necessários para investigação de crimes cibernéticos, ativamente reforçar a cooperação internacional em direção de combate á cibercrime e garantias de segurança cibernética, elaborar os cursos iniciais e de requalificação de especialistas em proteção de informação.[25]

A organização em Kyiv nos dias 14 e 15 de Junho de 2017 do Primeiro Encontro Global de Segurança Cibernética confirmou, que experiência de profissionais ucranianos em questões de proteção do ciberespaço poderia ser útil para a comunidade internacional.

Bibliografia

[1]. Internet trends 2017. Disponível na Internet em < URL: http://www.kpcb.com/internet-trends
[2]. The Global Risks Report 2017. Disponível na Internet em < URL: http://www3.weforum.org/docs/GRR17_Report_web.pdf
[3]. European Cybercrime Center – EC3. Disponível na Internet em < URL: https://www.europol.europa.eu/about-europol/european-cybercrime-centre-ec3
[4]. O perito prevê o aumento do número de crimes cibernéticos financiados pelo Estado. Disponível na Internet em < URL: http://www.securitylab.ru/news/485310.php
[5]. NATO: os ataques a aliança estão realizados por Estados. Disponível na Internet em < URL: http://ua.korrespondent.net/world/3815528-nato-kiberataky-na-alians-zdiisnuiuit-derzhavy

[6]. UK´s Trident nuclear submarines "vulnerable to catastrophic hack". Disponível na Internet em < URL: https://www.theguardian.com/uk-news/2017/jun/01/uks-trident-nuclear-submarines-vulnerable-to-catastrophic-hack-cyber-attack
[7]. Russia has developed a cyberweapon that can disrupt power grids. Disponível na Internet em < URL: https://www.washingtonpost.com/world/national-security/russia-has-developed-a-cyber-weapon-that-can-disrupt-power-grids-according-to-new-research/2017/06/11/b91b773e-4eed-11e7-91eb-9611861a988f_story.html?utm_term=.e19194733f58
[8]. Strengthening protection of critical infrastructure against terrorist attacks. Disponível na Internet em < URL: https://documents-dds-ny.un.org/doc/UNDOC/GEN/N17/038/61 /PDF/ N1703861.pdf?OpenElement
[9]. Decreto do Presidente da Ucrânia N.º 96/2016 Sobre decisão do Conselho de Segurança Nacional e Defesa da Ucrânia de 27 de Janeiro de 2016) "Sobre estratégia de segurança cibernética da Ucrânia" Disponível na Internet em < URL: http://www.president.gov.ua/documents/962016-19836
[10]. O Decreto do Presidente da Ucrânia N.º 32/2017 Sobre decisão do Conselho de Segurança Nacional e Defesa da Ucrânia" de 21 de Dezembro de 2017 "Ameaças á segurança cibernética do Estado e medidas de emergência para combatê-las". Disponível na Internet em < URL : http://www.president.gov.ua/documents/322017-21282
[11]. Disponível na Internet em < URL: http://www.itu.int/en/action/cybersecurity/Pages/gca.aspx
[12]. Mídia: milhões de computadores são vulneráveis a WannaCry. Disponível na Internet em < URL: http://ua.korrespondent.net/world/3850634-zmi-miliony-kompuiteriv-urazlyvi-pered-WannaCry
[13]. O vírus WannaCry atingiu o sistema informático do principal operador ferroviário na Alemanha. Disponível na Internet em < URL: http://nv.ua/ukr/world/countries/virus-wanna-cry-vraziv-sistemi-osnovnogo-zaliznichnogo-operatora-nimechchini-1137166.html
[14]. Produtora "Renault" atacada por hackers. Disponível na Internet em < URL: https://www.vectornews.net/news/world/24688-kompanyu-renault-atakuvali-hakeri.html
[15]. Nova onda de ataques cibernéticos. O vírus WannaCry atingiu milhares de computadores em países asiáticos. Disponível na Internet em < URL: http://tyzhden.ua/News/192285
[16]. Virus WannaCry: o dano estimado em um bilhão de dólares. Disponível na Internet em < URL: http://ua.korrespondent.net/world/3855174-virus-WannaCry-zbytok-otsinyly-v-miliard-dolariv
[17]. Internet Facilitated Organized Crime Assessement 2016

Disponível na Internet em < URL: https://www.europol.europa.eu/activities-services/main-reports/internet-organised-crime-threat-assessment-iocta-2016
[18]. Disponível na Internet em < URL: http://www.arcyber.army.mil/Pages/ArcyberHome.aspx
[19]. Disponível na Internet em < URL: https://www.unian.ua/science/2003241-zbitki-vid-ataki-virusu-petyaa-syagayut-8-milyardiv-dolariv-ekspert.html
[20]. United Nations Convention against Transnational Organized Crime and the Protocols Thereto. Disponível na Internet em < URL: https://www.unodc.org/unodc/en/treaties/CTOC/
[21]. European Convention on Mutual Assistance in Criminal Matters. Disponível na Internet em < URL: https://rm.coe.int/16800656ce
[22]. Convention on Cybercrime. Disponível na Internet em < URL: http://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/185
[23]. A Ucrânia assinou o acordo de cooperação com a Eurojust. Disponível na Internet em < URL: https://tsn.ua/politika/ukrayina-pidpisala-ugodu-pro-spivrobitnictvo-z-yevroyustom-680835.html
[24]. Hutsalyuk M.V. *A melhoria da legislação em vigor em questões de combate a criminalidade cibernética e sustentabilidade de segurança cibernética*, Informática legal – 2017 - N.º 2 (21) – 99-107 pp.
Disponível na Internet em < URL: http://ippi.org.ua/sites/default/files/14_3.pdf
[25]. Hutsalyuk M.V. *Metodologia de proteção da informação. Manual de estudo*. – 2ª edição, redigida e com adições. – Kyiv: Alterpress, 2011, 308pgs.